Refine Search

Search Results -

Terms	Documents
L3 and (707/10).ccls.	34

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L8

Refine Search | Recall Text | Clear | Interrupt

Search History

DATE: Friday, April 15, 2005 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
DB=USPT; THES=ASSIGNEE; PLUR=YES; OP=OR			
L8	L3 and 707/10.ccls.	34	L8
L7	L3 and 707/3.ccls.	27	L7
L6	L3 and 707	101	L6
L5	L3 and ((email or e$mail).ab.)	6	L5
L4	L3 and outlook	1	L4
L3	L2 and ((search$4 or query$4) with organization)	209	L3
L2	L1 and (select$4 with (individu$4 or address))	25931	L2
L1	(message or (email or e$mail) with instant)	134248	L1

END OF SEARCH HISTORY

Tips and Tricks for Outlook98

By Rick Paquin

The tips and tricks contained herein for Outlook98 define some of the methods for sharing information and data when used with Exchange Server. Some of these functions may not work properly without the use of Exchange Server. Also, these methods are contingent on the type of installation configuration you have on your computer. Some of the standard configurations and considerations that you should know prior to attempting to share data have been summarized within this article. Net Folders, which performs sharing functions that are very mail intensive will not be discussed.

Mail Basics You Should Know as an Outlook User

When Outlook was installed on your machine, the installer determined if your mail and other data would reside in a PST file (on your machine) or on a server (if Microsoft Exchange Server was used). It's important to know where your mail data is stored in order to provide backup files on a regular basis.

You cannot assume that the server is retaining your Outlook mail if you are employing Exchange Server on your network. Open Outlook and choose TOOLS/SERVICES and select DELIVERY to determine where your mail is actually being retained. If PERSONAL FOLDERS is selected, then your Outlook data is saved in one large file on your machine. With a PST extension your mail is not retained at the server level. If MAILBOX "your name" is selected, then your Outlook data is saved on the Exchange Server along with other Outlook data.

Caution: If you decide to store your Outlook mail in the PST file on your machine, you become responsible for your mail along with other Outlook data. If for some reason your PST file becomes corrupt, Exchange Server may not have a copy of your data or mail. Normally, all mail is erased from the server when it's downloaded to your computer. This means that you should be performing routine backups on your local PST file. Because these PST files can get quite large, you can also export specific folders in your PST file to separate PST files for backup purposes. Exporting any of the folders (calendar, contacts, tasks, inbox, etc.,) to it's own file creates a much smaller PST file that can be easily backed up to a floppy (if the file does not exceed the capacity of the disk).

If you don't have the means to properly backup your Outlook PST file, talk to your network administrator about enabling the server to store your data in your server MAILBOX.

Special Mail Sharing

Note: Use of Exchange Server is required for this function.

You can perform all sharing and joint functions via your MAILBOX folders or with PUBLIC folders (See PUBLIC folders below). The situation of sharing differs depending on whether you actively use a local PST file or a MAILBOX folder for your mail storage.

Scenario one - You do not use a PST file on your system to retain your data. All your mail, calendar and task data resides on the server.

From within Outlook, select FOLDER LIST. Click on the right hand mouse key on any Mailbox folder and select PROPERTIES. You'll notice a tab for PERMISSIONS. Using this feature, you can give others permission to view, post, edit and/or create from any default folder in your mailbox. If you give permission to a coworker, they will only have access to the folder you wish them to share.

The other users can connect to your mailbox in Outlook by selecting FILE/OPEN/OTHER USER'S FOLDER, and selecting your name from the Global list. They then must select the folder you have permitted them to share. You can create additional folders in your MAILBOX folder, however, only the default folders can be shared by others.

Scenario two - You use a PST file on your system to retain your data, and there are no public folders on the server.

Because you employ the use of a local PST file on your system, your MAILBOX folders will not contain data. Data is normally forwarded to your local PST file when you log into Outlook. If you want someone to view your new mail while you are out of the office, simply establish sharing permission levels on the properties of your INBOX located in your MAILBOX folders. This is the location where your mail resides when you are not logged into Outlook.

Provided you do not log onto your machine, other users you choose will have access to your new mail. Upon your return, as soon as you log into Outlook, all the new mail in your MAILBOX folders is then downloaded to your local PST file and erased from the server.

Users connect to your mailbox in Outlook by selecting FILE/OPEN/OTHER USER'S FOLDER, and selecting your name from the global list. They must select the folder (INBOX) which they have permission to view.

Public Folders

PUBLIC folders enable users to share Outlook data without the requirement to open someone's private mailbox using the FILE/OPEN command. PUBLIC folders exist in a separate category of the folder list. It also permits the creation of SHARED folders in addition to the default Outlook folders (CALENDER, NOTES, INBOX, etc.).

The primary difference between a PUBLIC folder and a MAILBOX folder is that the shared data can be contained in any named folder. That folder name is advertised to everyone in the PUBLIC folder list.

In scenario one above, you can create and share a PUBLIC folder or share a MAILBOX folder from your private mailbox. Similar sharing capabilities exist for joint functions, but Outlook restricts user clients to opening only the standard default folders.

Unless other users know that you have a shared MAILBOX, they do not see it advertised on the server. It may be desired not to publicize certain shared office data. If so, MAILBOX folders lend themselves better to that requirement.

PUBLIC folders lend themselves well to advertising information to a large organization where the folders themselves may change on a day to day basis. It's like a bulletin board system where the advertising of the shared folders is as important a function as the information itself.

In a large organization, the generation of primary level folders may get out of hand if everyone is permitted to generate primary folders. The administrator may choose to limit the creation of new folders to only when requested. Once the administrator creates a folder, rights can be assigned to everyone or limited to only those that need access to the folder.

Consider the situation where OFFICE61 needs a shareable folder for only themselves. The network administrator can provide a folder called OFFICE61, whereby only OFFICE61 users will be able to view its contents or create additional subfolders. Generation of sub folders may then be permitted to the group itself.

With PUBLIC folders, (provided you have proper rights) you can create a shareable folder that will be advertised to everyone on the server under the category PUBLIC folders. Users wishing to access this shared information can scroll down the list of PUBLIC folders to select the folder, without the requirement to open that folder. If they do not have permission to view the folder, they will get an appropriate warning message.

Sharing Other Outlook Data

Outlook's sharing methods differ depending on whether or not the product is used in conjunction with Exchange Server, and if you're using Exchange Server, it further depends on where you keep that data.

If the data you wish to share resides only on your hard drive, and not the server, you have certain considerations for access because you cannot directly share your PST file with someone else. Exchange Server has various options for sharing data.

Check with your network administrator to establish a public folder that you can control. Sharing elements of your Outlook data is as simple as opening FOLDERS VIEW and moving (dragging) a copy of your calendar, mail, tasks, etc. to your assigned PUBLIC folder.

Note: The act of moving or placing a copy of any portion of your private Outlook data to PUBLIC folders may remove password constraints. Upon moving a copy of your folder to a PUBLIC folder, immediately check properties and permissions to establish proper access control.

Although this PUBLIC folder will be advertised to everyone on the server, only those you provide access will be permitted to open the data element. PUBLIC folders permit you to continue using that folder for updates while others are also sharing its use.

Your MAILBOX folders on the server can also be shared easily with anyone. Go to FOLDER VIEWS and drag a copy of any folder you desire to have shared into one of the existing folders in your MAILBOX folder area.

Note: These folders will be empty because you're using a local PST file instead of the server for your Outlook data. Unfortunately only the default MAILBOX folders can be shared with other clients. Click the right mouse key and select properties on the MAILBOX folder you desire to share. Now choose PERMISSIONS and extend permission to any desired member.

Because you are using your private MAILBOX folders, they will not appear on the FOLDER LIST to other users. You must tell others you have them shared and they will have to use the FILE/OPEN command to connect to OTHER USERS FOLDER.

Note: You have only placed a copy of your data in the server MAILBOX to be shared. When you make additional changes to your CALENDER, TASK, etc., that you intend to be shared, make sure you are connected to the correct shared folder on the server.

You can share calendar appointments with others. Click INVITE ATTENDEES when creating a new appointment. This sends a request via e-mail to the people you chose. When they receive the message invitation, if they accept the request at their end, then it will automatically update their calendar with your appointment data.

If you want to be aware of the schedules of other members, they can invite you to their new appointments. Thus, by accepting their mail

announcements, it automatically updates your calendar to reflect everyone else's schedule.

Contact sharing can be performed through the mail. If you want to share a contact with another office member, after you add a contact to your contact database, you can hit the right mouse key and forward it to other mail recipients.

You can tag a group of contacts and forward them via mail to other office members. They can then move them directly into their CONTACTS folder by dragging them individually or as a group over to your CONTACTS folder or your Outlook bar, where they will automatically be added without any further intervention.

If you wish to share your Outlook data with other users while you are away and your server does not have PUBLIC folders, you must copy the data you want to share from your local PST to your MAILBOX folders on the server. Once your data has been copied to one of your existing MAILBOX folders, access the folder's properties and adjust the permission properties for those who need to have access to your data.

Joint Scheduling

If you are a manager for an office where a joint schedule would be desired, start by setting up a shared calendar on Exchange server in either your MAILBOX or PUBLIC folders. If you are creating a new calendar in PUBLIC folders, see the previous paragraphs regarding user rights in PUBLIC folders.

You may desire to start a common office calendar for joint scheduling. You can share your MAILBOX folder with others in the office, but it MUST be one of the original default folders.

If all your calendar data resides on Exchange Server as CALENDAR, and it contains data you do not want shared, copy that calendar data to CALENDAR2, so that the default CALENDAR can be shared without the data you do not want shared.

Creating a shared calendar in PUBLIC folders is easy. You can create one from scratch by selecting the primary folder you have appropriate rights to (for example, OFFICE61) and select FILE, NEW, FOLDER. You must select the type of folder, which for a calendar will be APPOINTMENTS.

Let's say you already have a calendar with your schedule in your local PST file. You can simply drag a copy of your personal calendar down to the OFFICE61 folder under PUBLIC folders.

Note: The act of moving or placing a copy of any portion of your private Outlook data in PUBLIC folders may remove all password constraints. Upon moving a copy of your folder to a PUBLIC folder, immediately check properties and permissions of that folder to establish proper access control.

No matter what method you use to create your new public calendar, you should immediately establish the properties for your calendar, including the rights of others to post, view or manage it. Click the right hand mouse key on the calendar and you'll see a wide array of management features, including detailed permission options for your users.

Generally, as creator of the CALENDER, you have full rights to perform all functions, but other users who post to your CALENDER will only have rights to their own postings. This safeguards others from tampering with another's schedule or posting.

For example: Sally can place her schedule entries on the CALENDER; Joe can place his there as well. Sally cannot change Joe's entries, and Joe cannot change Sally's. As owner you have full control over all content and can also establish read or write privileges for each user as needed.

You can import scheduling data from other private CALENDERS when users already have their future schedules developed.

You may have others that have already placed their schedules in their personal Outlook PST file and you would like to merge their schedules into your calendar.

With PUBLIC folders:
- Have the other user copy his calendar data to a PUBLIC CALENDAR folder. Then import the data from their shared CALENDAR into your CALENDAR.

Without PUBLIC folders:
- Use MAILBOX folders to share data. Other users must share their calendar data with you from their MAILBOX CALENDAR. Once you have access to the shared CALENDAR, import the data from their shared CALENDAR into your CALENDAR.

When you're adding entries to the joint office calendar follow the guidelines below if you would like those appointments to appear in your private calendar:

Open the Joint Calendar. Add a new appointment and invite others. There's a block at the top of the appointment screen that lets you invite others.

Click on the invite others block and select yourself from the global list of user names. If you would like your schedule to appear on other users' calendars, invite them also. Once you've created your appointment, select Save and Close. You will then be asked if you want the invitation sent to the others as well. Select OK.

A message will be sent to you with a request to accept the appointment. By accepting it, Outlook will add it to your private primary calendar.

The other users you selected for your appointment request will also receive a similar invitation. The invitation, when accepted, will generate an automatic confirmation back to the originator of the invitation.

About the Author:

Searched for http://www.chips.navy.mil/archives/99_jul/outlook.htm **16** Results

* denotes when site was updated.

Search Results for Jan 01, 1996 - Apr 13, 2005

1996	1997	1998	1999	2000	2001	2002	2003	2004	2005
0 pages	0 pages	0 pages	0 pages	0 pages	5 pages	3 pages	4 pages	4 pages	0 pages
					Mar 05, 2001 *	Jan 15, 2002	Jan 04, 2003	Jan 15, 2004	
					Apr 26, 2001 *	Feb 21, 2002	Jul 02, 2003	Mar 08, 2004	
					Sep 22, 2001 *	Nov 29, 2002 *	Aug 26, 2003	Jun 03, 2004	
					Nov 13, 2001		Oct 26, 2003	Oct 29, 2004	
					Nov 23, 2001				

Office Resource Kit
Office Admin Update Center

Update Libraries
Office 2003 Administrative Updates
Office XP Administrative Updates
Office 97-2000 Administrative Updates

Related Web Sites
Product Support
Office Community
Office Developer Center

Worldwide
Office Worldwide

Customizing the Outlook 98/2000 E-mail Security Update

Help

Assistance > Deployment Center Assistance > Office Admin Update Center > Office 97-2000 Administrative Updates

If your organization is using Microsoft Outlook® 98/2000 with a server that has server-side security, such as Microsoft Exchange Server, you can customize the security update to meet your organization's needs. For example, you can help control the types of attached files blocked by Outlook, modify the Outlook Object Model warning notifications, and specify user or group security levels.

At this time, to enable custom security settings, your clients must be using Outlook with Microsoft Exchange Server and have either the Mailbox (MDB) or Offline folders (OST) as their default e-mail delivery location. You cannot modify the settings if a client is using a local .Pst file for a mailbox, or if you are using Outlook with a third-party e-mail service. Microsoft has been working with other third-party e-mail services to provide them with the appropriate documentation that would enable them to offer this level of customization. In particular, Lotus has agreed to enable this level of customization and Hewlett-Packard and Novell are currently evaluating. In cases where you cannot customize the settings, the default settings in the security update will be applied to your Outlook installation.

Warning Lowering any default security setting may increase your risk of virus execution or propagation. Use caution and read the documentation before you modify these settings.

Obtaining the Outlook E-mail Security Update and administrative tools

General information on the Outlook 98/2000 E-mail Security Update and links to the downloadable files are available on the Office Update Web site. This site includes a series of articles on virus protection settings, the types of files restricted in e-mail messages, and software from independent software vendors that may be affected by the update. For more information, see Outlook 2000 SR-1 E-mail Security Update International Releases on the Office Update Web site.

Administrative tools for the Outlook E-mail Security Update are available from the Office Resource Kit Web site. The administrative tools consist of three files, packaged into one self-extracting executable:

- OutlookSecurity.oft is an Outlook template that enables you to customize the security settings on the Microsoft Exchange server.
- Readme.txt is a document that provides information on the values and settings available in the template and describes how to deploy the new settings on Exchange Server.
- Outlk9.adm is an updated system policy file that is required for client computers that have been set up with system policies.

Toolbox To download the administrative tools for the Outlook E-mail Security Update, see **Outlook 2000 SR-1a Security Update Administrative Tools** in the Office Resource Kit Toolbox. You can find this downloadable file on the Office 2000 Resource Kit Downloads page.

Note When using the Outlook E-mail Security Update with Outlook 2000, you must first install Office 2000 Service Release 1a (SR-1a) before you can modify the default security settings.

The following sections describe how to customize the Outlook E-mail Security Update and how to deploy these customized settings to client computers.

Customizing the Outlook E-mail Security Update

You can modify the default values for the Outlook E-mail Security Update by using the Outlook Security template to configure specific settings on Exchange Server. The Outlook Security template is an Outlook Item Template that you run through Microsoft Outlook. The template contains two tabs, one for Outlook Security Settings and one for Programmatic Settings. When you first load the template, the settings show the default values for the Outlook E-mail Security Update.

Before you begin to modify the security settings, you must create a public folder named "Outlook Security Settings" on Exchange Server. The administrator must create this folder, using that exact name, in the root folder of the Public Folder tree. You must set the folder Access Control Lists (ACL) so all users can read all items in the folder. However, only those users who you want to be able to create or change security settings should have permission to create, edit, or delete items in the folder. After you create the folder, you can use the template to make the changes you need.

To use the Outlook Security template to modify settings on Exchange Server

1. Download the Outlook 2000 SR-1a Security Update administrative tools and copy them to a working directory on your computer.

2. On a computer running Outlook, open OutlookSecurity.oft from the file system.
3. When asked to select a folder, select the **Outlook Security Settings** public folder you created on Exchange Server. The template will then open in Compose mode.
4. On the **Tools** menu of the template, point to **Forms**, and then click **Publish Form**. (The folder selected should be your current folder, Outlook Security Settings.)
5. In the **Form Name** box, type "Outlook Security Form".
6. Click the **Publish** button. The security template is now published in the Security Settings folder.
7. Close the form, and when prompted to save changes, click **No**.
8. In the **Folder** List, right-click the **Outlook Security Settings** folder, and then click **Properties** on the shortcut menu.
9. In the **When posting to this folder, use** list, click **Outlook Security Form**, and then click **OK**.
10. Click the **New** button to open up a new security template.
11. Create either a default security setting or custom settings for a specific set of users.

    Details on all fields and settings in the template can be found in the file Readme.txt, included with the administrative tools download.

Deploying customized Outlook e-mail security settings to client computers

After you configure the security update on Exchange Server, you must enable the customized settings for your users. To enable the changed settings, you deploy a new registry key to the client computers. How you deploy the registry key depends upon whether Microsoft Office was initially deployed with system policies.

- If Office was deployed with system policies, you must change the policies on Exchange Server.

  This involves removing the current .Adm file and replacing it with the new one from the download. The new .Adm file will automatically pass your customized security settings to client computers each time users log on to the system.

- If Office was deployed without system policies, you must modify a registry key directly on the client computers.

  Outlook will respect this new registry key, even if you are not using policies.

Note Different procedures are required to update policies under Windows® 2000 and the Windows® 95/98 or Windows NT® 4.x operating systems. Make sure to use the appropriate procedures for your system.

To update the Outlook policy template file under Windows 2000

1. From the **Start** menu, choose **Run**, then type **gpedit.msc** to start the Group Policy editor.
2. Expand the following series of folders:
   User Configuration\Administrative Templates
3. Right-click **Administrative Templates**, then click **Add/Remove Templates**.
4. In the **Add/Remove Templates** dialog box, select Outlk9, then click the **Remove** button to remove the old template.
5. Click the **Add** button, then browse to the folder where you installed the updated Outlk9.adm template. Select the file name and click the **Add** button to add the new template to the folder.
6. Click the **Close** button.
7. Expand the following series of folders:
   User Configuration\Administrative Templates\Microsoft Outlook 2000\Tools|Options\Security
8. Double-click the **Outlook virus security settings** policy name.
9. In the **Properties** dialog box, select the **Enabled** option, then select the check box for **Apply individual settings for Outlook virus security**.
10. Click the **Apply** button to apply the new policy, then click **OK** to close the **Properties** dialog box.

To update the Outlook policy template file under Windows 95/98 or Windows NT 4.x

1. From the **Start** menu, choose **Run**, then type **poledit.exe** to start the System Policy editor.

   The System Policy Editor is included with the Office Resource Kit core tool set.

2. From the **Options** menu, choose **Policy Template**.
3. In the Policy Template Options list, select the entry for Outlk9.adm, then click the **Remove** button.
4. In the same dialog box, click the **Add** button, then browse to the directory where you installed the updated Outlk9.adm template. Select the file name and click **Open** to add the new template to the folder.
5. Click **OK** to close the dialog box.
6. From the **File** menu, choose **Open Registry**, then double-click the **Local User** icon.
7. In the **Properties** dialog box, expand the following series of folders:
   Microsoft Outlook 2000\Tools|Options\Security
8. Select the check box for **Outlook virus security settings**, then select the box on the lower-half of the dialog box for **Apply individual settings for Outlook virus security**.

9. Click **OK** to apply the new policy and close the dialog box.

If you are using Exchange Server but are not using system policies in your organization, you can distribute the new registry key directly to the client computer. Registry key files are a registered file type, which means that the key will be automatically installed on a client computer when a user double-clicks the file name.

To create a new registry key for distribution to client computers

1. Start the registry editor and expand the following subkey:

   HKEY_CURRENT_USER\Software\Policies\Microsoft\Security.

2. From the **Edit** menu, choose **New**, then click **DWORD value** to add a new registry key. The value name for the key must be **CheckAdminSettings**.
3. Select the new key name, then from the **Registry** menu choose **Export Registry File.**
4. In the **Export Registry File** dialog box, type a name for the registry file and select the option for **Selected Branch** under the **Export Range** group. Click **Save** to create the registry file. Registry files have a .Reg extension.

To distribute the new key to client computers, you can add it to a log-in script, copy it to a shared server for users to run, or attach it as a shortcut to an e-mail message. You cannot attach the file itself to a message, since .Reg files are restricted by the Outlook E-mail Security Update.

Related links

For more information about the Outlook 98/2000 E-mail Security Update, Search the Knowledge Base for the following articles.

Article Q263275 - OL97: Outlook E-mail Security Update Not Available for Outlook 97.

Article Q262617 - OL98: Information About the Outlook E-mail Security Update.

Article Q262618 - OL98: Known Issues with the Outlook E-Mail Security Update

Article Q262700 - OL98: Developer Information About the Outlook E-mail Security Update.

Article Q263296 - OL98: Administrator Information About the Outlook E-mail Security Update.

Article Q262631 - OL2000: Information About the Outlook E-mail Security Update.

Article Q262634 - OL2000: Known Issues with the Outlook E-Mail Security Update.

Article Q262701 - OL2000: Developer Information About the Outlook E-mail Security Update.

Article Q263297 - OL2000: Administrator Information About the Outlook E-mail Security Update.

Please let us know if this content was helpful.

Rate this content:

☆☆☆☆☆

Tell us why you rated the content this way (optional):

650 characters maximum

Submit

Printer-friendly version